CLAIMS

What is claimed is:

1. A method for determining secure endpoints of tunnels in a network that uses Internet security protocol, the method comprising the computer-implemented steps of :

sending from a first network device a first description of network traffic that is to be protected;

receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected;

creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic; and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic.

2. A method as recited in Claim 1, wherein the first description comprises a first set of proxies, wherein the second description comprises a second set of proxies, and wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of proxies and the second set of proxies.

3. A method as recited in Claim 1, wherein the first description comprises a first protocol and the second description comprises a second protocol, and further comprising the steps of determining a third protocol for the third description based on determining a logical intersection of the first protocol and the second protocol.

4. A method as recited in Claim 3, wherein determining the third protocol comprises the steps of:

determining that the third protocol is IP when both the first description and the second description identify IP as a protocol;

determining that the third protocol is a specific protocol when the first description identifies IP and the second description identifies the specific protocol;

determining that the third protocol is a specific protocol when both the first description and the second description identify the same specific protocol.

5. The method as recited in Claim 1, wherein the first description comprises a packet summary value that summarizes packets in the network traffic to be protected, and wherein the second description is generated by the second network device based on comparing the packet summary value to one or more access control lists that are managed by the second network device.

6. The method as recited in Claim 1, wherein the first description of network traffic comprises a packet summary that includes:

IP protocol information that is associated with the network traffic emanating from a source end host, wherein the source end host is associated with the first network device;

port information that is associated with the source end host;

port information that is associated with a destination end host, wherein the destination end host is associated with the second network device;

an IP address that is associated with the source end host;

an IP address that is associated with the destination end host; and

a proxy address of the source end host;

wherein the second description is generated by the second network device based on comparing the packet summary to one or more access control lists that are managed by the second network device.

7. The method as recited in Claim 1, further comprising the step of:

determining, at the second network device, whether the packet summary matches a security policy information that is associated with the second network device;

wherein the packet summary is associated with the first description of network traffic.

8. The method as recited in Claim 1, wherein the second description of network traffic comprises a response that includes:

IP protocol information that is associated with the network traffic emanating from a destination end host, wherein the destination end host is associated with the second network device;

an IP address that is associated with the second network device; and

proxy addresses that are associated with a destination end host.

9. The method as recited in Claim 8, wherein the proxy addresses that are associated with the destination end host include a first subnet that includes the destination end host and a second subnet that includes a source end host, wherein the source end host is associated with the first network device.

10. The method as recited in Claim 1, wherein deriving a third description of network traffic further comprises the step of:

determining based on the first description of network traffic and the second description of network traffic a first intersection proxy comprising protocol information;

determining based on the first description of network traffic and the second description of network traffic a second intersection proxy comprising port information; and

determining based on the first description of network traffic and the second description of network traffic a third intersection proxy comprising proxy address information.

11. The method as recited in Claim 1, further comprising the steps of:

receiving at the first network device an IP packet from a source end host that is associated with the first network device;

verifying that the IP packet falls within the third description of network traffic.

12. A method as recited in Claim 1, wherein the first description comprises a first port value and the second description comprises a second port value, and further

comprising the steps of determining a third port value for the third description based on determining a logical intersection of the first port value and the second port value.

13. A method as recited in Claim 12, wherein determining the third port value comprises the steps of:

determining that the third port value is a specific port value when both the first description and the second description identify the same specific port value;

determining that the third port value is a specific port value when one of the first description and the second description identify the specific port value.

14. A computer-readable medium carrying one or more sequences of instructions for determining secure endpoints of tunnels in a network that uses Internet security protocol, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

sending from a first network device a first description of network traffic that is to be protected;

receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected;

creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic; and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic.

15. A computer-readable medium as recited in Claim 14, wherein the first description comprises a first set of proxies, wherein the second description comprises a second set of proxies, and wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of proxies and the second set of proxies.

16. A computer-readable medium as recited in Claim 14, wherein the first description comprises a first protocol and the second description comprises a second protocol,

and further comprising the steps of determining a third protocol for the third description based on determining a logical intersection of the first protocol and the second protocol.

17. A method for establishing a secure connection between two network devices, the method comprising the computer-implemented steps of:

receiving, at a second network device and from a first network device, a first description of network traffic that is to be protected;

in response to receiving the first description of network traffic, creating and sending to the first network device a second description of network traffic that is to be protected;

receiving at the second network device a third description of network traffic that is to be protected from the first network device based on a logical intersection of the first description of network traffic and the second description of network traffic; and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic.

18. A computer-readable medium carrying one or more sequences of instructions for establishing a secure connection between two network devices, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, at a second network device and from a first network device, a first description of network traffic that is to be protected;

in response to receiving the first description of network traffic, creating and sending to the first network device a second description of network traffic that is to be protected;

receiving at the second network device a third description of network traffic that is to be protected from the first network device based on a logical intersection of the first description of network traffic and the second description of network traffic; and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic.

19. An apparatus for determining secure endpoints of tunnels in a network that uses Internet security protocol, comprising:
means for sending from a first network device a first description of network traffic that is to be protected;
means for receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected;
means for creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic; and
means for establishing the secure connection between the first network device and the second network device based on the third description of network traffic.

20. An apparatus for determining secure endpoints of tunnels in a network that uses Internet security protocol, comprising:
a network interface that is coupled to the network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
sending from a first network device a first description of network traffic that is to be protected;
receiving, at the first network device and from a second network device, a second description of network traffic that is to be protected;
creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic; and

establishing the secure connection between the first network device and the second network device based on the third description of network traffic.